UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/526,169	11/17/2005	Chin Shyan Ooi	7404P001	6494

8791 7590 02/10/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/526,169	OOI ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7-17,19,21-24 and 27-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,7-17,19,21-24 and 27-30* is/are rejected.

7)☒ Claim(s) *1,7,10 and 16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 October 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 22 October 2008, has been entered into record. In this amendment, claims 1, 3-5, 7-17, 19, 21-24, and 27-30 have been amended, and claims 2, 6, 18, 20, 25, 26 have been cancelled.

2. Claims 1, 3-5, 7-17, 19, 21-24, and 27-30 are presented for examination.

Response to Arguments

3. As to the objections to the drawings: The applicant has submitted replacement drawings, and the examiner hereby withdraws the objections.

4. As to the rejection of claims 16-18 under 35 USC 112: The applicant has submitted amendments, and the examiner hereby withdraws the rejection.

5. Applicant's arguments filed 22 October 2008 have been fully considered but they are not persuasive.

As to claims 1, 16, and 19, it is argued by the applicant that Brandys does not disclose a portable data storage device arranged to generate at least one key and to encrypt the generated key using a secret key that is permanently stored in the portable storage device. The examiner respectfully disagrees. It is noted that in the previous office action dated 6/23/08 on page 10, the examiner notes that the element "generated key is transmitted in a form encrypted using a secret key which is permanently stored in the portable storage device, the portable storage device further being arranged to verify a digital signature generated by the host using the generated key and the requested data" is not taught by Brandys. This element includes the recitation "arranged to verify

a digital signature..." which is not stated in the applicant's argument. Brandys discloses that a message digest (i.e. at least one key) is created and is encrypted with the private key (i.e. secret key) (page 4, lines 19-21), and the private key is stored in a tamper-resistant component on the smart card (i.e. permanently stored) (page 4, lines 2-3).

As to claim 1, it is argued by the applicant that Brandys and Buch do not disclose a device that transmits data requested by a host. The examiner respectfully disagrees. It is noted that the examiner has interpreted the smart card as the portable device. Brandys discloses that when the biometric data analyzer of the smart card receives biometric data from a user (i.e. request), the public key is transmitted (page 3, line 3, page 4, lines 1-4). Brandys also discloses that non-volatile memory of the smart card stores information such as the public key (page 7, lines 8-12).

As to claim 1, it is argued by the applicant that Brandys and Buch do not disclose a portable data storage device arranged to receive from the host a digital signature based on the generated key and the requested data for use in verifying that the requested data has been correctly received by the host. The examiner respectfully disagrees. Buch discloses that the public key is used to decrypt the digital signature, which can be used to verify if hash values match, indicating that the correct sender is the originator (i.e. data correctly received) (0028, lines 10-13).

Specification

6. The abstract of the disclosure is objected to because "[Fig. 1]" in line 11 should be removed. Correction is required. See MPEP § 608.01(b).

Claim Objections

7. Claims 1, 7, 10, and 16 are objected to because of the following informalities:

a. In claim 1, lines 3, 4 and 5: "data" is unclear if it relates to "data" (claim 1, line 2);

b. In claim 1, line 10: "at least one key" is unclear if it relates to "at least one key" (claim 1, line 7);

c. Claim 7 is dependent on claim 6, which has been canceled. It is believed by the examiner that claim 7 should be dependent on claim 1, and it has been treated as such for the remainder of this office action.

d. In claim 10, line 2: "data" is unclear if it relates to "data" (claim 1, line 3);

e. In claim 16, lines 4 and 5: "data" is unclear if it relates to "data" (claim 16, line 3);

f. In claim 16, line 10: "at least one key" is unclear if it relates to "at least one key" (claim 16, line 7);

g. In claim 16, line 18: "a command" is unclear if it relates to "a command" (claim 16, lines 8-9).

Appropriate correction is required.

Drawings

8. The drawings were received on 22 October 2008. These drawings are acceptable.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 3-5, 7-9, 11-13, 15-17, 19, 21-24, and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brandys (WO 02/073877 A2) in view of Buch et al. (US 2003/0217165 A1 and Buch hereinafter).

As to claims 1 and 16, Brandys discloses a system and method for authenticating users and data, the system and method having:

a portable data storage device including a non-volatile memory to store data (page 7, lines 8-12);

an interface section to receive data from and transmit data to a host (page 4, lines 3-4);

a master control unit to transfer data to and from the non-volatile memory (page 4, lines 2-3; page 10, lines 25-26);

integrated circuit for generating at least one key (page 4, lines 1-2);

the portable data storage device being arranged, upon receiving a command (i.e. biometric data from user) **from the host requesting the data stored in the non-volatile memory, to generate at least one key** (i.e. message digest)**, to encrypt the generated key using a secret key** (i.e.

private) **that is permanently stored in the portable storage device and to transmit the encrypted key** (i.e. digital signature) **and the requested data stored in the non-volatile memory to the host using the interface section** (page 3, line 35; page 4, lines 1-4, 17-23);

a host computer, the host computer being arranged to transmit a command to the portable data storage device using the interface section to request the data (page 4, lines 17-18).

Brandys does not disclose:

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data for use in verifying that the requested data has been correctly received by the host.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as evidenced by Buch.

Buch discloses a system and method for end-to-end authentication of session initiation protocol messages using certificates, the system and method having:

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data for use in verifying that the requested data has been correctly received (i.e. received from correct sender) **by the host** (0028, lines 5-8).

Given the teaching of Buch, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Buch by creating a key in order to verify a digital signature. Buch recites motivation by disclosing that verifying a signature can be used to authenticate a sender and confirm the integrity of a message (0005, lines 10-16). It is obvious that the teachings of Brandys would have benefited from the teachings of Buch by providing a key with which to verify a digital signature in order to authenticate a sender and verify the integrity of a message.

As to claim 19, Brandys discloses:

the portable data storage device receiving and instruction (i.e. biometric data from user) **from the host requesting the data stored in a non-volatile memory of the portable data storage device** (page 4, lines 1-4; page 7, lines 8-12);

the portable data storage device generating at least one key (page 4, lines 1-2);

the portable data storage device encrypting the generated key using the secret key permanently stored in the portable data storage device (page 4, lines 2-3, 20-21);

the portable data storage device obtaining the requested data from the non-volatile memory and the portable data storage device transmitting

to the host the requested data and the encrypted key (page 3, line 35; page 4, lines 1-4, 17-23);

the host decrypting the encrypted key using the secret key permanently stored in the host (page 6, line 18). The examiner asserts that it would have been well known to one of ordinary skill in the art at the time the invention was made to use either symmetric keys, where the same key is used from encryption and decryption, or asymmetric keys for encryption/decryption because they are functionally equivalent.

the host generating a digital signature based on the decrypted key and the requested data (page 6, lines 19-21).

Brandys does not disclose:

the host transmitting the digital signature from the host to the portable data storage device;

the portable data storage device using the digital signature to verify that the requested data has been correctly received by the host.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as evidenced by Buch.

Buch discloses:

the host transmitting the digital signature from the host to the portable data storage device (i.e. callee client) (0028, lines 1-5);

the portable data storage device using the digital signature to verify that the requested data has been correctly received (i.e. received from correct sender) **by the host** (0028, lines 5-8, 10-13).

Given the teaching of Buch, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Buch by using a transmitted signature to verify data. Please refer to the motivation recited above in respect to claims 1 and 16 as to why it is obvious to apply the teachings of Buch to the teachings of Brandys.

As to claims 3 and 22, Brandys discloses:

wherein the digital signature is produced by hashing the received data to generate a hash result, and encrypting the hash result using the generated key (page 4, lines 19-23).

As to claims 4 and 23, Brandys discloses:

wherein the generated key is the private key of a public key/private key pair (page 4, lines 1-3).

As to claims 5 and 24, Brandys discloses:

wherein the verification of the digital signature is performed in the portable data storage device using the public key (page 5, line 35).

As to claims 7 and 27, Brandys discloses:

wherein the requested data includes both data present in the non-volatile memory, and also biometric data obtained from a biometric sensor of the portable data storage device (page 2, lines 24-26).

As to claims 8 and 28, Brandys does not disclose:

the requested data is transmitted from the portable data storage device to the host in an encrypted form.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as evidenced by Buch.

Buch discloses:

the requested data is transmitted from the portable data storage device to the host in an encrypted form (0027, lines 14-15).

Given the teaching of Buch, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Buch by transmitting encrypted data. Buch recites motivation by disclosing that if a message is encrypted, a private key is needed in order to decrypt the message (0028, lines 13-16), providing message security. It is obvious that the teachings of Buch would have improved the teachings of Brandys by transmitting encrypted data so that only a private key can be used to acquire the original message, thus providing message security during transmission.

As to claims 9 and 29, Brandys discloses:

a biometric sensor (page 3, lines 14-15)**;**

a verification engine for granting access to data stored in the portable data storage device based on a biometric verification of the user's identity by comparison of biometric data received using the biometric sensor with pre-stored biometric data (page 2, lines 24-26)**.**

As to claim 11, Brandys does not disclose:

the interface section include a USB connector and a USB interface device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as evidenced by Buch.

Buch discloses:

the interface section include a USB connector and a USB interface device (0019, lines 11-13)

Given the teaching of Buch, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Buch by allowing connectively through USB. Buch recites motivation by disclosing that various interfaces may be used (0019, lines 11-14). It is obvious that the teachings of Buch would have improved the teachings of Brandys by providing for an interface using USB because various interfaces may be used to connect to the system bus.

As to claim 12, Brandys does not disclose:

> **the connector is a USB plug integral with the portable data storage device.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as evidenced by Buch.

Buch discloses:

> **the connector is a USB plug integral with the portable data storage device** (0018, lines 8-17).

Given the teaching of Buch, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Buch by providing for a USB connection for the device. Please refer to the motivation recited above in respect to claim 11 as to why it is obvious to apply the teachings of Buch to the teachings of Brandys.

As to claim 13, Brandys discloses:

> **the interface section is for wireless communication with the host** (page 3, lines 11-12).

As to claim 15, Brandys discloses:

> **a camera for generating image data, and/or a microphone for capturing audio data** (page 7, lines 19-20)**, the master control unit being arranged to store the image data and/or the audio data in the memory** (page 7, lines 8-12).

As to claim 17, Brandys discloses:

> **wherein the generated key is one key of a public key/private key pair** (page 4, lines 1-3)**, and the host is arranged to generate a digital signature using the private key and the requested data** (page 6, lines 19-21).

11. Claims 10 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brandys in view of Buch as applied to claims 1 and 19 above, and further in view of Iwagaki et al. (US 2003/0161468 A1 and Iwagaki hereinafter).

As to claims 10 and 30, Brandys in view of Buch does not disclose:

> **a compression algorithm for exploiting any redundancy in data received by the portable data storage device to compress it before storing it in the non-volatile memory, and a decompression engine to regenerate the data before it is transmitted from the portable data storage device.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Buch, as evidenced by Iwagaki.

Iwagaki discloses a system and method for securing a storage device, the system and method having:

> **a compression algorithm for exploiting any redundancy in data received by the portable data storage device to compress it before storing it in the non-volatile memory, and a decompression engine to regenerate**

the data before it is transmitted from the portable data storage device (0009, lines 13-17).

Given the teaching of Iwagaki, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Buch with the teachings of Iwagaki by providing for compression and decompression of stored data. Iwagaki recites motivation by disclosing that data can be very large and storing uncompressed data in a storage device does not effectively utilize the storage capacity of the device (0009, lines 9-12). It is obvious that the teachings of Iwagaki would have improved the teachings of Brandys in view of Buch by allowing for the compression and decompression of stored data in order to use the storage capacity of the device more effectively.

12. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brandys in view of Buch as applied to claim 1 above, and further in view of Fang (US Patent 6,536,941 B1).

As to claim 14, Brandys in view of Buch does not disclose:

a housing, the housing including a narrowed end for use as a pointer.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Buch, as evidenced by Fang.

Fang discloses a wrist-worn personal flash disk apparatus, the apparatus having:

a housing, the housing including a narrowed end for use as a pointer (33, Figure 1).

Given the teaching of Fang, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Buch with the teachings of Fang by providing for a housing with a narrowed end. Fang recites motivation by disclosing that the storage device can have multiple functions depending on the physical shape of the device (Abstract, lines 1-14). It is obvious that the teachings of Fang would have improved the teachings of Brandys in view of Buch by providing for a specific shaped housing, such as a narrowed end, in order to allow for multiple functions of the device.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431